UF Workstation Guidelines for Users of Restricted Data

Who Should Know This

These guidelines apply to anyone with access to UF Restricted Data from their workstation.

Definitions

Workstation A computer designed primarily to be used by one person at a time.

Purpose

These guidelines are intended to establish workstation safeguards to protect the confidentiality of Restricted Data.

Guidelines

1. Avoid storing Restricted Data on workstations. Where no reasonable alternative exists:
    a. First obtain permission from the Data Principal [3].
    b. Minimize the amount of Restricted Data stored.
    c. Minimize the length of time the Restricted Data is stored on the workstation.
    d. Position your display screen containing Restricted Data in such a way as to minimize unauthorized view.
    e. Ensure your workstation is physically secure when left unattended.
    f. Activate workstation locking software or log out any time you step away from the workstation.
2. Before using Restricted Data on a workstation, consult your Unit Information Security Manager or local IT support staff [1,3] for:
    a. Approved workstations.
    b. Secure configuration and maintenance [4].
    c. Inactivity timeout configuration.
    d. Secure backup requirements [5].
    e. Encryption requirements.
3. Lost or stolen workstations used with Restricted Data must be immediately reported to the Data Principal and the UF Privacy Office [4], usually through the User's supervisor, so that necessary steps can be taken to limit damage and liability.
4. Restricted Data on workstations that are being replaced or retired must be destroyed [6]. The user is responsible, but should consult their Unit Information Security Manager or local IT support staff for destruction requirements.
5. The following safe computing practices should be followed.
    a. Use strong passwords that are difficult to guess, but easy to remember. Protect your password like you would protect your credit card.
    b. Do not use computer features that remember or auto-complete your password.
    c. Ensure any workstation used for with Restricted Data has current updates. Select the automatic update option if available.
    d. Ensure any workstation used with Restricted Data has current anti-virus protection. Configure automatic updates if available.
    e. Configure an inactivity time-out that requires a password for re-entry. The time-out period must not exceed 15 minutes.

Bibliography

[1] UF Acceptable Use Policy: http://www.it.ufl.edu/policies/aupolicy.html
[2] UF IT Security Policy: http://www.it.ufl.edu/policies/security/
[3] UF IT Standards for Confidentiality of Restricted Data: http://www.it.ufl.edu/policies/security/uf-it-sec-data.html
[4] UF IT Network and Host Security Standard: http://www.it.ufl.edu/policies/security/uf-it-sec-network.html
[5] UF Guidelines for IT Workers to Protect Restricted Data on Backup Media: http://www.it.ufl.edu/policies/security/documents/ITworker_draft/backups.pdf
[6] Media Reuse and Data Destruction Standard: http://www.it.ufl.edu/policies/security/documents/ITworker_draft/disposal.pdf